

# THREAT MODELING

---

Planning digital security for your story

Jonathan Stray

Columbia Journalism School

ONA 2013

# Journalism Security Disasters

## Hacked accounts and sites

AP

Washington Post

New York Times

...

## Sources exposed

Vice reveals John McAfee's location

AP phone records subpoena

Filmmaker's laptop seized in Syria

...

## Data leaked

Wikileaks cables archive was not meant to be public

...

# What are we protecting?

There are basically two things we want to protect: information and computers.

## Information not protected

- someone reads your secret email
- source identity exposed
- story draft leaked

## Computer not protected

- someone erases your hard drive
- Twitter account hacked
- site down

# Three important messages

1. Journalism is high-risk profession
2. Even if you're not working on a sensitive story,  
you are a target
3. For sensitive stories, you need a plan.

# Two types of security practice

Even if you are not working on a sensitive story, you are a target if your colleagues are working on a sensitive story.

So we need to think about two things:

- What everyone in the newsroom should be doing
- What you need to do for a specific story

# What everyone needs to know

- Use strong passwords and 2-factor authentication
- Recognize phishing
- Encrypt your drive

# Passwords

1. Don't use a common password. Avoid words in the dictionary.
2. Use two-factor authentication
3. Consider passphrases, and password management tools like 1Password
4. If you use the same password for multiple sites, your password is only as strong as the security on the weakest site.

plaintext	frequency
password	32027
123456	25969
12345678	8667
1234	5786
qwerty	5455
12345	4523
dragon	4321
pussy	3945
baseball	3739
football	3682
letmein	3536
monkey	3487
696969	3345
abc123	3310
mustang	3289
michael	3249
shadow	3209
master	3182
jennifer	2581
111111	2570
2000	2550
jordan	2538
superman	2523
harley	2485
1234567	2479
fuckme	2378
hunter	2377
fuckyou	2362

LinkedIn  
from June 2012 breach

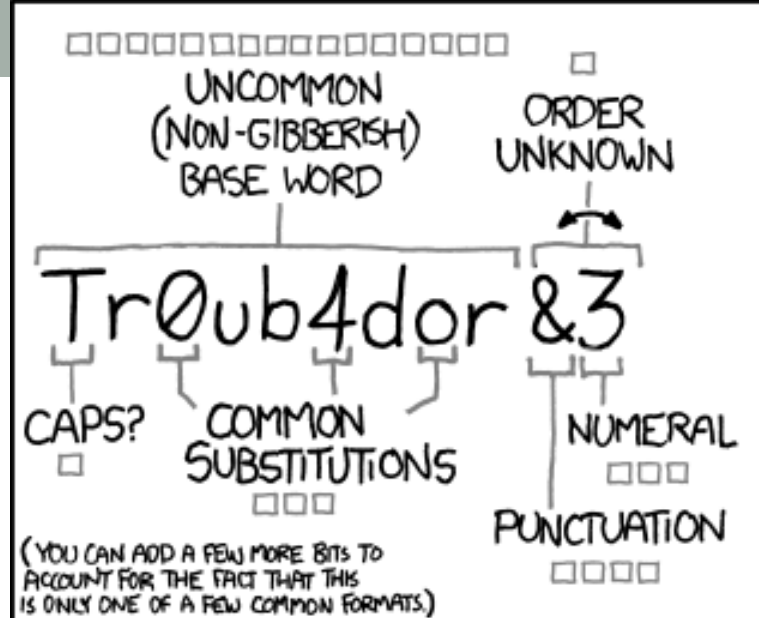
```

2516 123456
2188 password
1205 12345678
696  qwerty
498  abc123
459  12345
441  monkey
413  111111
385  consumer
376  letmein
351  1234
318  dragon
307  trustno1
303  baseball
302  gizmodo
300  whatever
297  superman
276  1234567
266  sunshine
266  iloveyou
262  fuckyou
256  starwars
255  shadow
241  princess
234  cheese
231  123123
229  computer
225  gawker
223  football
204  blahblah

```

Gawker  
from Dec 2010 breach





~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

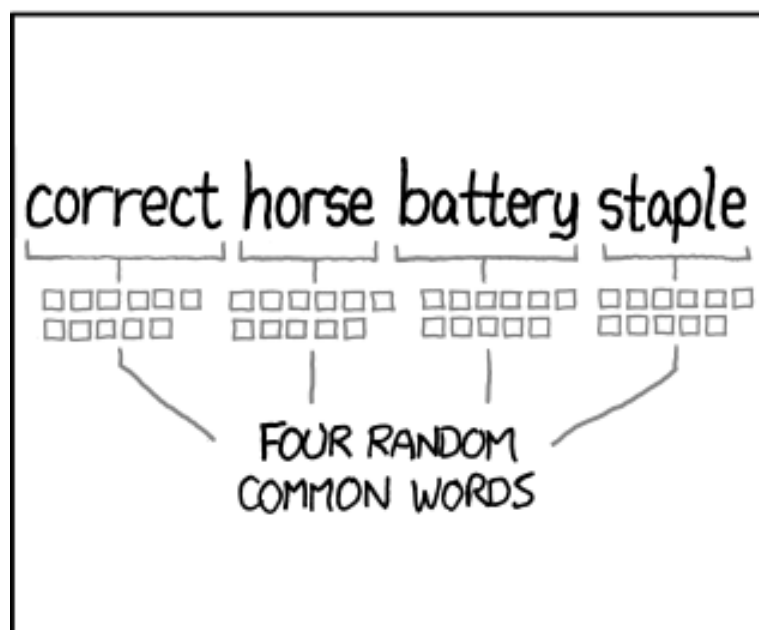
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Two-factor authentication

## 2-step verification

Help keep the bad guys out of your account by using both your password *and* your phone.

Get Started



"something you know, plus something you have"  
password + phone

# Phishing

By far the most common attack against journalists (or maybe anyone.) Relies on getting the user to visit a site under false premises.

Typically directs users to a fake login page to trick them into entering passwords. But: more sophisticated attacks exist that work just by viewing page.

Protection: beware suspicious links! Especially those that take you to a login page!

**Read the URL *before* clicking a link from a message.**  
***Always* read the URL before typing a password.**

## Example of a typical, poorly-constructed phishing e-mail message

**From...** UTSA MAINTENANCE <maintenace@utsa.edu>  
**To...** John Doe  
**Cc...**  
**Subject:** MAINTENANCE ALERT!!

Dear Email User,

Prior to the unwanted spam in our UTSA webmail service, we have decided to perform mentainance on our site. Our mentainance is based on free Anti-spamming protection for all UTSA users account, which is number 10 of our UTSA email/exchange terms and condition. You are to send in your information below in this order.

\*\*\*\*\*

1.) Full NAME:  
2.) USER ID:  
3.) PASSWORD:  
4.) ALTERNATE EMAIL:  
5.) SECRET QUESTION:  
6.) SECRET ANSWER:  
7.) DATE OF BIRTH:

\*\*\*\*\*

This process will help us to fight against spam mails. Failure to submit your UTSA email/exchange Account Details, will render your email address in-active from our database.

NOTE: You will be notifield in your email password reset message immediately after undergoing this process for security reasons.

Technical System Team

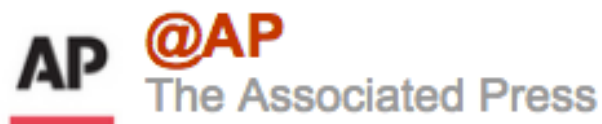
MAINTENANCE TEAM  
[maintenance@utsa.edu](mailto:maintenance@utsa.edu) <mailto:maintenance@utsa.edu>

**misspelled words / poor grammar**

**Reputable organizations / companies will NEVER ask for your password**

**E-mail address should be "Office of Information Technology"**

# AP Twitter hacked by phishing



 Follow @AP

Breaking: Two Explosions in the White House and Barack Obama is injured

April 23, 2013 5:07 pm via web [Reply](#) [Retweet](#) [Favorite](#)

# AP phishing email

Sent: Tue 4/23/2013 12:12 PM

From: [An AP staffer]

Subject: News

Hello,

Please read the following article, it's very important :

<http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/>

[A different AP staffer]

Associated Press

San Diego

mobile [removed]

The link didn't really go to washingtonpost.com!

# Read the URL before you click!

The image is a screenshot of a web browser displaying a Bloomberg news article. The browser's address bar shows the URL [www.bloomberg.com/news/2013-06-30/fbi-s-data-mining-needs-scrutiny-too.html](http://www.bloomberg.com/news/2013-06-30/fbi-s-data-mining-needs-scrutiny-too.html). The article title is "FBI's Data Mining Needs Scrutiny, Too" by Rachel Levinson-Waldman, dated June 30, 2013. The article text discusses the NSA's database of phone records and the FBI's data mining activities. On the right side, there is a "Reader Submissions" section with several article titles. At the bottom of the browser window, a URL is highlighted with a pink oval: [www.bloomberg.com/news/2013-06-06/nsa-said-to-collect-millions-of-verizon-phone-records.html](http://www.bloomberg.com/news/2013-06-06/nsa-said-to-collect-millions-of-verizon-phone-records.html). The text "ssments pay" is partially visible at the end of this URL.

**FBI's Data Mining Needs Scrutiny, Too**  
By Rachel Levinson-Waldman | Jun 30, 2013 3:00 PM PT

We recently [learned](#) that the National Security Agency has a database with the records of almost every phone call made in the U.S. To address public concerns over its surveillance activities, the agency has begun to explain how it uses the [metadata](#) -- information including when calls are made, how long they last and to whom they are placed -- it has accumulated over the last seven years.

Although Americans deserve this explanation, they shouldn't delude themselves. Even if the NSA's controversial program were shut down tomorrow, another government agency that is busy collecting and retaining personal data would keep humming along. True accountability for the government's surveillance activities should also include an airing of -- and tighter restrictions on -- the Federal Bureau of Investigation's power to collect and store substantial amounts of innocuous information about Americans.

Since 2008, for instance, the FBI has had the authority to conduct "assessments" -- investigations that require no suspicion of criminal activity. In service of these [low-level investigations](#), an FBI agent may use various invasive methods, including infiltrating public meetings of groups as diverse as the American Civil Liberties Union or Alcoholics Anonymous, using informants, and even putting the target of the investigation under full-time physical surveillance.

**Reader Submissions**  
Submit a column to Bloomberg View

**Margaret Carlson»**  
**Boehner to Tea Party: Shut Yourself Down**

**Cass R. Sunstein»**  
**For Obama and Boehner, Weakness Is Strength**

**Richard Holden & Justin Wolfers»**  
**Nobel Prize Shows Both Wisdom and Madness of Crowds**

**Ramesh Ponnuru»**  
**Yellen Shouldn't Apologize for Helping Wall Street**

**Jeffrey Goldberg»**  
**The Rise and Fall of Israel's Settlement Movement**

[www.bloomberg.com/news/2013-06-06/nsa-said-to-collect-millions-of-verizon-phone-records.html](http://www.bloomberg.com/news/2013-06-06/nsa-said-to-collect-millions-of-verizon-phone-records.html) ssments pay


# Increasingly sophisticated phishing

“ The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you. ”


Spear phishing = selected targets, personalized messages







# But all is not lost, if you are alert



**James Ball**  
@jamesrbuk









 Follow

The guys doing the Guardian phishing attack I mentioned yesterday (it's SEA) are really very good: sustained, changing, mails today.

 Reply  Retweet  Favorite  More

**9**  
RETWEETS

**2**  
FAVORITES



2:12 AM - 29 Apr 13

# Defending against phishing

- Be suspicious of generic emails
- Read the URL before you click
- *Always* read the URL before typing in a password
- Report suspicious links to your security people

# Secure storage

We're assuming you have some "data" you want to protect.  
Documents, notes, photos, interviews, video...

But also: stored passwords, information about your  
colleagues, ability to impersonate you (e.g. fake emails)

# Laptop falls into Syrian govt hands, sources forced to flee

The Syrians had interrogated McAllister about his activities, and seized his laptop, mobile phone, camera, and footage. All of McAllister's research was now at the disposal of Syrian intelligence. When Kardokh heard that McAllister had been arrested, he didn't hesitate—he turned off his mobile phone, packed his bag, and fled Damascus, staying with relatives in a nearby town before escaping to Lebanon. He said that other activists who had been in touch with McAllister fled the country as well, and several of those who didn't were arrested. "I was happy that I hadn't put him in contact with more people," Kardokh said.

# Securing your storage

How many copies are there?

- The original file might be on your phone, camera SD card, etc.
- What about backups and cloud syncing?
- Use secure erase products

Could they get a copy?

- steal your laptop
- walk into your office at lunch
- take your camera at the border

If they had a copy, could they read it?

- Encrypt your whole disk!
- Use TrueCrypt (Windows), FileVault (Mac), LUKS (Linux)

# For sensitive stories, have a plan

Security doesn't just happen.  
It requires careful planning and meticulous habits.

There is no such thing as "secure."  
There is only "secure against a particular threat."

# Threat modeling

## **What do I want to keep private?**

(Messages, locations, identities, networks...)

## **Who wants to know?**

(story subject, governments, law enforcement, corporations...)

## **What can they do?**

(eavesdrop, subpoena... or exploit security lapses and accidents)

## **What happens if they succeed?**

(story's blown, legal problems for a source, someone gets killed...)

# What do I want to keep private?

## Which data?

- emails and other communications
- photos, footage, notes
- your address book, travel itineraries...

## Privacy vs. Anonymity

- Encryption protects *content* of an email or IM, not the identity of sender and recipient
- Do you *also* need to keep these identities secret?
- Anonymity is very hard, requires special tools and meticulous habits.



# Adversaries: who wants to know?

Most of the time, the NSA is not the problem.

Your adversary could be a government, the subject of a story, another news organization...

# What can they do? Types of attacks

## Technical

- hacking, intercepted communications, code-breaking

## Legal

- lawsuits, subpoenas, detention

## Social

- phishing, "social engineering," exploiting trust

## Operational

- that one time you didn't use a secure channel

## Physical

- theft, installation of malware, network taps, torture

# Defend yourself with technology

## Communications

- PGP (secure email)
- CryptoCat, OTR (secure messaging)
- Tor (anonymity)

## Password Management

- 1Password, LastPass, Keepass

## Disk encryption

- TrueCrypt (Windows), FileVault (Mac), LUKS (Linux)

# Defend yourself with law

In the U.S. the Privacy Protection Act prevents police from seizing journalist data without a warrant...

...if the data is on your premises.

If it's in the cloud, no protection!

Know the law. Have a lawyer and a legal strategy.

# What are you risking?

Security is never free. It costs time, money, and convenience.

Sometimes security measures can make it difficult or impossible to get a story. So "how much" security do you need? It depends on what you risk.

- blown story
- arrested source
- dead source

# Threat modeling scenario #1

You are a photojournalist in Syria with digital images you want to get out of the country. Limited internet access is available at a cafe. Some of the images may identify people working with the rebels who could be targeted by the government if their identity is revealed. In addition you would like to remain anonymous until the photographs are published, so that you can continue to work inside the country for a little longer, and leave without difficulty.

# Threat modeling scenario #2

You are working on an investigative story about the CIA conducting operations in the U.S., in possible violation the law. You have sources inside the CIA who would like to remain anonymous. You will occasionally meet with these sources in but mostly communicate electronically. You would like to keep the story secret until it is published, to avoid pre-emptive legal challenges to publication.

# Threat modeling scenario #3

You are reporting on insider trading at a large bank, and talking secretly to two whistleblowers. If these sources are identified before the story comes out, at the very least you will lose your sources, but there might also be more serious repercussions — they could lose their jobs, or the bank could attempt to sue. This story involves a large volume of proprietary data and documents which must be analyzed.



# Threat modeling scenario #4

You are working in Europe, assisting a Chinese human rights activist. The activist is working inside China with other activists, but so far the Chinese government does not know they are an activist and they would like to keep it this way. You have met the activist once before, in person, and have a phone number for them, but need to set up a secure communications channel.

# Security depends on practice

Sources, journalists, editors, staff must work together flawlessly.

Everyone needs to understand the security plan, and *what makes it secure*.

Then they must have meticulous habits. They must *never* do anything insecure.

Putting a plan into practice is often the hardest part.

# Case study: leaked cables

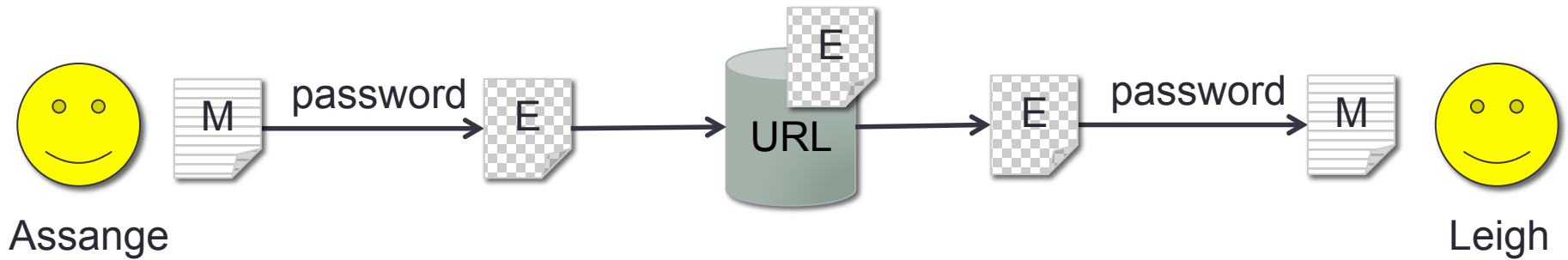
Julian Assange gave a password and a temporary URL to Guardian reporter David Leigh.

Leigh downloaded the file in encrypted form from the temporary URL.

Leigh decrypted the file and reported on the contents.

...but later, all the cables were available publicly, which is not what either Assange or Leigh intended.

# The Plan

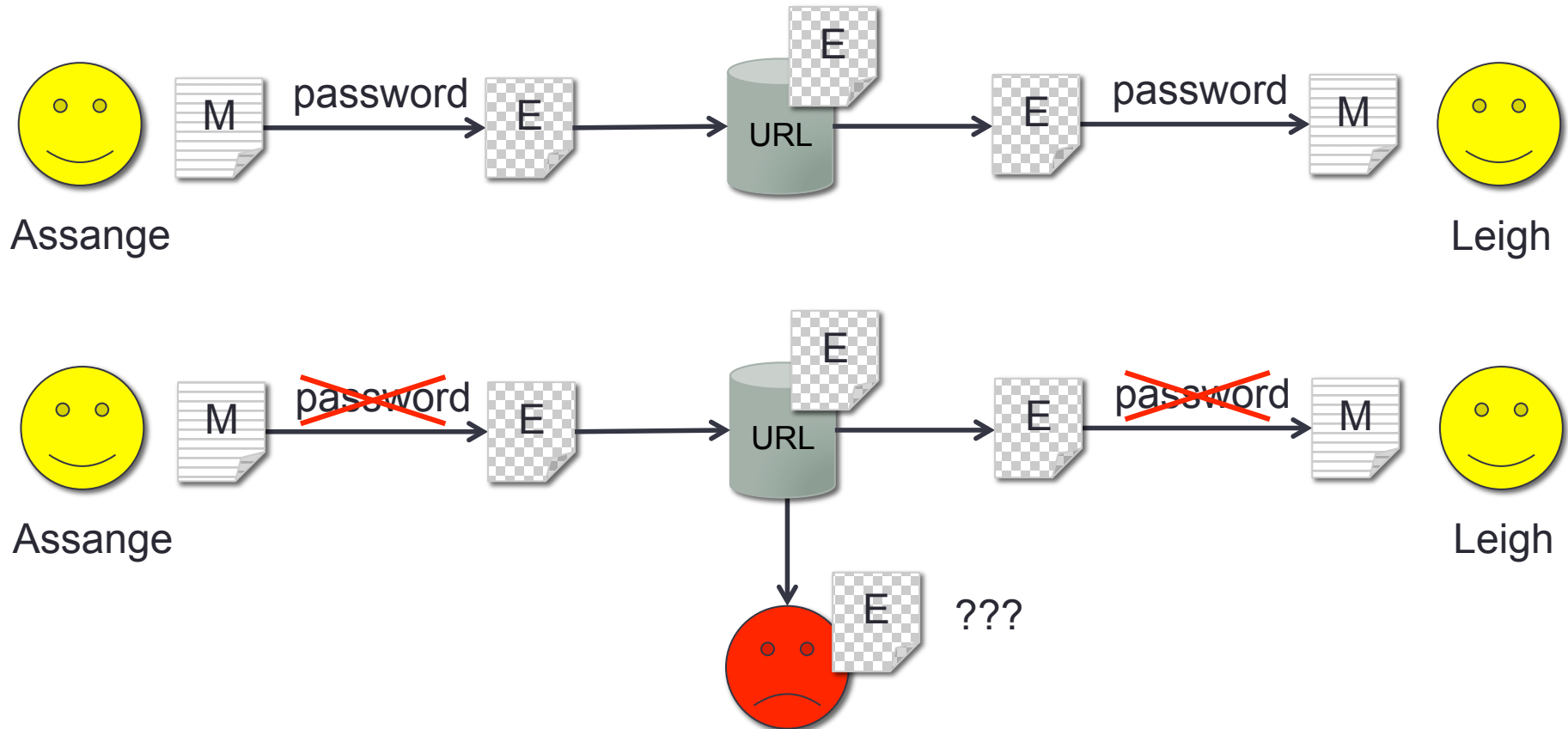


M = original message (file containing cables)

E = encrypted file

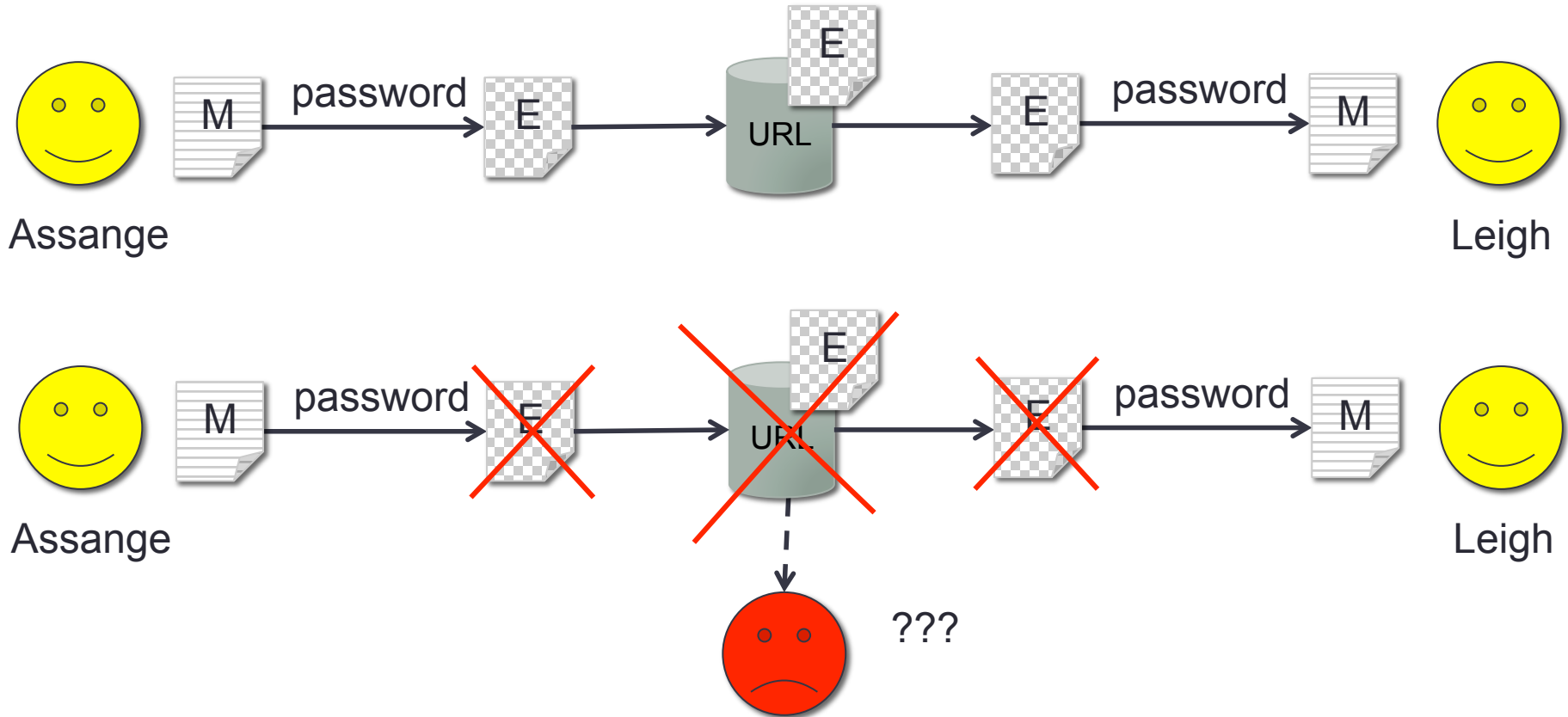
URL = server where encrypted file is stored

# What Assange was thinking



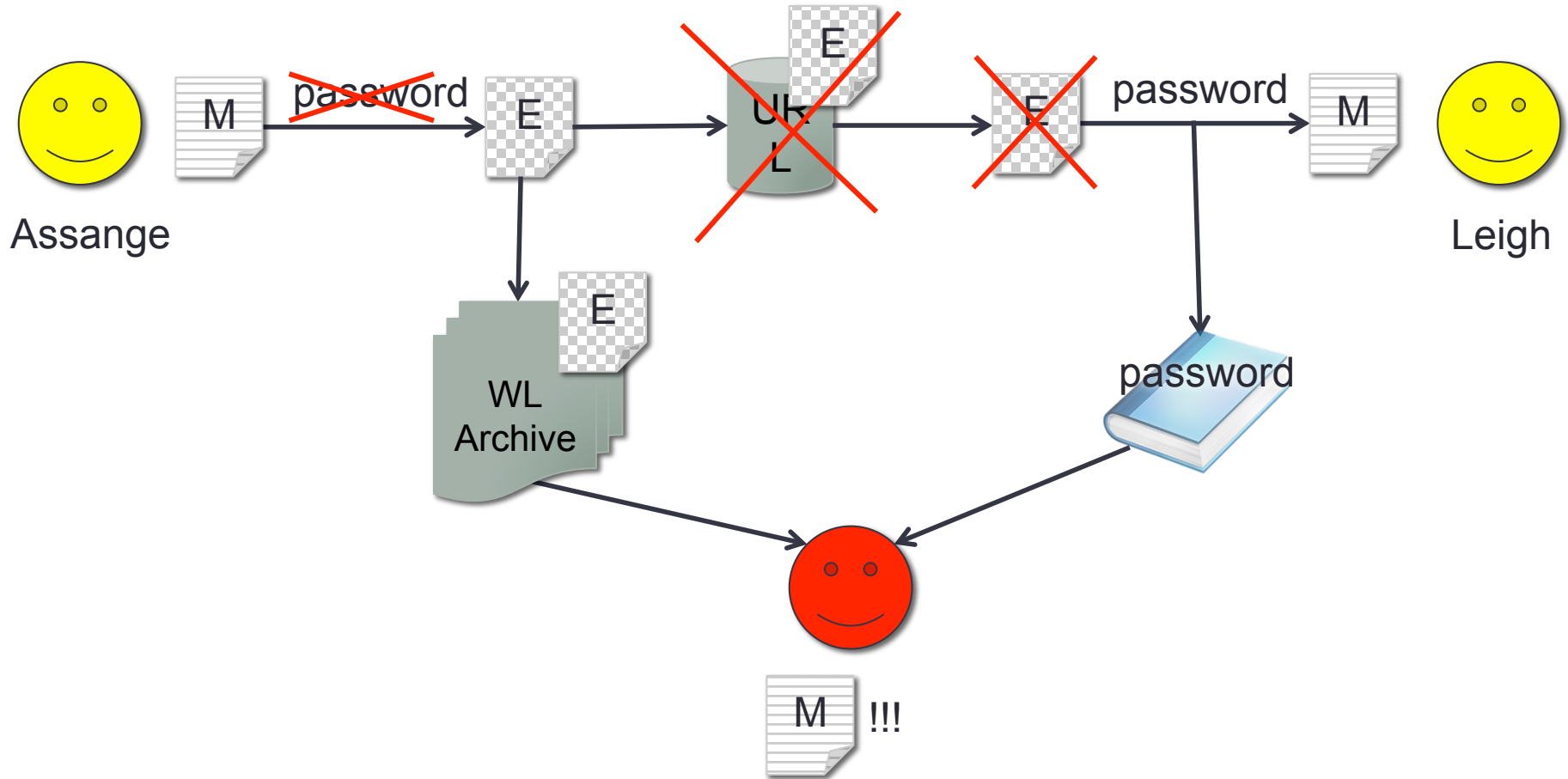
Assange thinks an attacker might get the encrypted file, but can't open it without the password

# What Leigh was thinking



Leigh thinks an attacker cannot get the file (because it is on a secret and temporary server) so it doesn't matter if he later publishes the password.

# What actually happened



The encrypted file is released (inadvertently?) in a public Wikileaks archive, while Leigh publishes the password in a book. Now attacker has both!

# Resources

Committee to Protect Journalists information security guide

<http://www.cpj.org/reports/2012/04/information-security.php>

Jen Valentino's Encryption and Operational Security for Journalists Hacks/Hackers presentation

<https://gist.github.com/vaguity/6594731>

[http://www.cjr.org/behind\\_the\\_news/hacks\\_hackers\\_security\\_for\\_jou.php?page=all](http://www.cjr.org/behind_the_news/hacks_hackers_security_for_jou.php?page=all)

Threat modeling exercise

<http://jmsc.hku.hk/courses/jmsc6041spring2013/2013/02/08/assignment-6-threat-modeling-and-security-planning/>